

# **Validation of a vignettes-based, hands-on cybersecurity threats situational assessment tool**

**Melissa Carlton**, Nova Southeastern University, FL, USA, [melissa.carlton.phd@gmail.com](mailto:melissa.carlton.phd@gmail.com)

**Yair Levy**, Nova Southeastern University, FL, USA, [levyy@nova.edu](mailto:levyy@nova.edu)

**Michelle M. Ramim**, Middle Georgia State University, GA, USA, [michelle.ramim@mga.edu](mailto:michelle.ramim@mga.edu)

## **Abstract**

*Advanced Persistent Threats (APTs) have been growing with social engineering and corporate e-mail compromise reported as the two most penetration vectors to organizational networks. Historically, users (i.e., office assistants, managers, executives) have access to sensitive data and represent up to 95% of cybersecurity threats to organizations. This study addressed the problem of threats to organizational information systems (IS) due to vulnerabilities and breaches caused by employees. While in the past, only selected employees at the organization had access to the computer networks, with the proliferation of mobile devices almost all employees and vendors/contractors have access to the organizational networks. Computer and mobile device users are one of the weakest links in the cybersecurity chain, due to their limited cybersecurity skills (CySs). Over the years, the measures of CySs of computer users were based on self-reported surveys or measured knowledge only. Prior IS and medical research found participants view scenarios as nonintrusive and unthreatening, while providing a realistic way to assess various situations from sexual harassment to chemical hazards. Therefore, this paper discusses the validation stage of a cybersecurity threats situational assessment tool that utilizes vignettes with observable hands-on tasks to measure and quantify CySs. Discussions and future research are also presented.*

**Keywords:** Cybersecurity skills, cybersecurity knowledge, cybersecurity experience, cybersecurity threats situational assessment tool, and advanced persistent threats mitigation.

## **Introduction**

Conducting daily operations, interacting, and sharing knowledge online is a part of everyday life, both professionally as well as personally. But, completing activities online does not come without risks and a potential for harm. Individuals, governments, and organizations are regularly reporting substantial financial as well as information losses due to vulnerabilities and breaches caused by insiders. Although advances in Information Technology (IT) have been substantial over the past several decades, when it comes to the protection of corporate information systems (IS), cybersecurity threats have continuously grown with social engineering and business e-mail compromise reported to be the two most growing penetration vectors to most organizations (Federal Bureau of Investigation (FBI), 2017). Without proper cybersecurity skills (CySs), employees, even those with the best of intentions, represent the weakest link in an organization's computer and network security. Skills are defined as the combination of knowledge, experience,

and ability to do something well (Boyatzis & Kolb, 1991). CySs correspond to the skills surrounding the hardware and software required to execute computer as well as network security to mitigate cybersecurity attacks (Boyatzis & Kolb, 1991; Carlton & Levy, 2015).

The demand for employees with skills to protect IS and the information contained with those systems continue to rise as cybersecurity attacks increase (U.S. Department of Labor, 2018). Vulnerabilities of individuals, organizations, and governments conducting transactions online are exploited by hackers with skills or with limited skills (Cox, 2015). Cybersecurity attacks appear to be an issue for all nations and go beyond borders. Many heads of states and country leaders have expressed their concerns about cybersecurity attacks happening to their governments, systems, and citizens. Furthermore, they indicated the significant need for people with CySs in their countries to ensure proper resilience for such attacks. For example, Benjamin Netanyahu, the Prime Minister of Israel, indicated that individuals with the proper CySs are “an essential condition for [our] national security and economic growth in the 21st century” (Globes, 2016). Similarly, the Prime Minister of the United Kingdom noted how important are individuals with proper CySs to protect his country (United Kingdom, 2015). Currently, there is a clear gap in what skills individuals demonstrate and what skills they need to protect themselves as well as their organizations for successful work performances (Levy & Ramim, 2017). Thus, this study builds on prior research conducted by Carlton and Levy (2015) as well as Carlton, Levy, Ramim, and Terrell (2015) that identified the top nine expert validated cybersecurity threats, the matching skills to mitigate the threats, and each skill’s importance weight, which is operationalized as a vignettes-based, hands-on cybersecurity threats situational assessment tool.

The main goal of this study was to provide further validity and reliability of the developed vignette-based, hierarchical hands-on cybersecurity threats mitigation situational assessment tool in preparation of gathering empirical data for measuring the cybersecurity skills levels (CySLs) of non-IT professionals. Furthermore, the measurement of computer and mobile device users’ CySLs addresses the problem of threats to organizational IS due to vulnerabilities and breaches caused by employees. Prior IS and medical research found participants view vignettes as nonintrusive and unthreatening. Therefore, this research study utilized the previously developed cyber threats situational assessment tool to ensure each participant’s response is accurately recorded by the tool.

The next section provides a brief review of literature as an insight into the body of knowledge that is related to cybersecurity threats, skills, and extant assessment tools. The research methodology adopted by this study is then explained, followed by an in-depth look into the importance of reliability and validity. This paper is concluded with a discussion of the results of the pilot study used to deem the vignettes-based, hands-on, cybersecurity threats situational assessment tool as valid.

## **Review of Literature**

Extant knowledge creation literature (e.g., Solek-Borowska, 2017) identified that an employee’s skills and competencies are imperative in the success of an organization. Whereas, the Internet is a highly effective tool in the sharing of knowledge (Paliszkiewicz, Svanadze, & Jikia, 2017). However, accessing the Internet does not come without its risks. Therefore, individuals should

have opportunities to encourage the sharing of lessons learned from cyber attacks to curtail the detrimental effect of such attacks (Solek-Borowska, 2017). Due to the interactivity of the vignettes-based, hands-on cybersecurity threats situational assessment tool, individuals may learn new knowledge that will enable them to develop skills without the fear of causing harm to personal or an organization's assets (Geri, Winer, & Zaks, 2017; Solek-Borowska, 2017).

During the developmental phase of this research project, the situational assessment tool was constructed to address the lack in literature of a vignette-based, realistic cybersecurity threats situational measure of computer and mobile device users' CySLs. Such skills are needed to mitigate security breaches of an individual's or corporation's IS (Carlton et al., 2015). Thus, the situational assessment tool allows researchers to "create knowledge grounded in data systematically derived from practice" (Richey & Klein, 2014, p. 1). According to Ellis and Levy (2009), developmental research is comprised of three major elements: 1) product criteria is established and validated; 2) process for product development is accepted and formalized; as well as 3) determination of the product's criteria is met through a formalized, accepted process. In the work of Tracey and Richey (2007), a systematic process was used to develop and then validate their model using the Delphi technique where a panel of subject matter experts (SMEs) analyzed along with offering feedback on the proposed design. After suggested revisions were analyzed and incorporated, their model was then validated by another Delphi technique cycle with the SMEs (Tracey, 2009; Richey & Klein, 2014). Thus, our study followed that same systematic process to provide robust hands-on measure.

## **Definition of Terms and Acronyms**

The following represent terms, definitions, and acronyms.

**Cybersecurity** – "A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems" (Cybersecurity Curricula 2017, 2017, p. 16).

**Cybersecurity skills (CySs)** – correspond to an individual's technical knowledge, ability, and experience surrounding the hardware and software required to execute IS security to mitigate cyber-attacks (Choi, Levy, & Hovav, 2013).

**Cybersecurity Skills Index (CSI)** – The cybersecurity skills index is a logical and repeatable quantitative measure that indicate the level of cybersecurity skills of an individual (Carlton & Levy, 2015; Carlton et al., 2015).

**Cybersecurity Skills Levels (CySLs)** – correspond to an individual's scores demonstrated through the vignettes-based, hands-on cybersecurity threats situational assessment tool.

**Information System (IS)** – "A discrete set of information resources [user included] organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information" (Kissel, 2013, p. 101).

**Information Technology (IT)** – "Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management,

movement, control, display, switching, interchange, transmission, or reception of data or information” (Kissel, 2013, p. 104).

**Personally identifiable information (PII)** – Any information about an individual that may be used to distinguish or trace an individual’s identity (e.g., name, date of birth, and/or social security number) (McCallister, Grance, & Scarfone, 2010).

**Work Information System (WIS)** – An information system operating in an organization, for example, an employee desktop, a shop point-of-sale computer, or a shared workstation at an organization.

## **Methodology**

In this section, we will outline some of the key processes needed for quality developmental research when it comes to ensure it is a robust research tool. Specifically, Ellis and Levy (2010) indicated that developmental research serves as a ‘bridge’ between industry and academic research to ensure that the research conducted is applied, while the instrument or artifact developed is valid and reliable. Moreover, Ellis and Levy (2010) indicated that:

“careful attention to establishing the reliability and validity of the methods employed in the study can significantly reduce the possibility that the results indicate something that is in fact not the case. The best way to establish the reliability and validity of the methods employed is to follow accepted processes and use established tools as they were designed to be used.” (p. 115)

The cybersecurity threats situational assessment tool we have developed is available either via mobile device as an application (app), or via the Web accessed by a browser. The tool itself is based on set of vignettes with observable hands-on tasks for each of the identified CySs, where each task within the tool was then scored, while the overall scoring was then calculated following the formula validated by the SMEs. To ensure validity and reliability of the tool, the following two sections will define and outline the meaning of reliability as well as validity processes undertaken. The work was done to ensure the cybersecurity threats situational assessment tool developed is indeed providing a robust tool to measure and quantify correctly the CySs.

## **Reliability**

Reliability ensures consistent or error-free results are produced (Rogers, 1995). It also makes “a statement about measurement accuracy” (Boudreau, Gefen, & Straub, 2001, p. 5). Reliability may exist without validity, but validity cannot exist without reliability (Mendoza, 2014; Reinard, 2006). Moreover, validity and reliability influence the amount a researcher may learn about the phenomenon under investigation (Leedy & Ormrod, 2013). An assessment tool’s reliability is determined by reproducibility and consistency (Helminen, Halonen, Rankinen, Nissinen, & Rauramaa, 1995). Without stability and internal consistency, the measurement precision of an assessment tool is viewed as weak (Helminen et al., 1995; Chakhssi, de Rulter, & Bernstein, 2010). Thus, this study evaluated the cybersecurity threats situational assessment tool, in addition to ensure the reliability of capturing the data collected (Onwuegbuzie, Bustamante, &

Nelson, 2010; Sheng, Magnien, Kumaraguru, Acquisti, & Cranor, 2007). Specifically, while the tool was developed using a scoring methodology on the tasks performed by the user, manual calculations were conducted in parallel using observing research assistants to count the scoring and compare them to the scoring calculated by the tool itself. This process is discussed as part of the results of this study below.

## **Validity**

Validity is the researchers' ability to "draw meaningful and justifiable inferences from scores about a sample or population" (Creswell, 2005, p. 600). A tool is considered valid based on its relevance and provision of an accurate assessment of what it is measuring (Alias, 2015). Incorporating the validation of a measure can help substantiate research findings, as well as "move the [research] forward toward meaningful replicated studies" (Straub, 1989, p. 162). Striving for validation, a panel of eight SMEs were asked how relevant each task was in accessing the respective skill and to describe in their own words revisions (if any) needed for the skill or task in a prior phase of this research project (Boudreau et al., 2001; Carlton et al., 2015; Nelson, Bustamante, Wilson, & Onwuegbuzie, 2008). Moreover, asking for computer and networking security experts' comments as well as suggestions ensured the cybersecurity threats situational assessment tool maintained consistency, 'state-of-the-art' realistic knowledge, and industry practicality (Ball, Ramim, & Levy, 2015; Wang, Nieveen, & van den Akker, 2007). Therefore, this study reduced the threat to the tool's validity by establishing the vignette-based, and using realistic cyber tasks that were validated through multiple rounds of an expert panel following the Delphi technique (Ramim & Lichvar, 2014; Carlton & Levy, 2015). Furthermore, eliciting the feedback from the SMEs ensured both validity and reliability that the criteria used to develop the assessment tool was appropriate (Brown, Levy, Ramim, & Parrish, 2015).

## **Results**

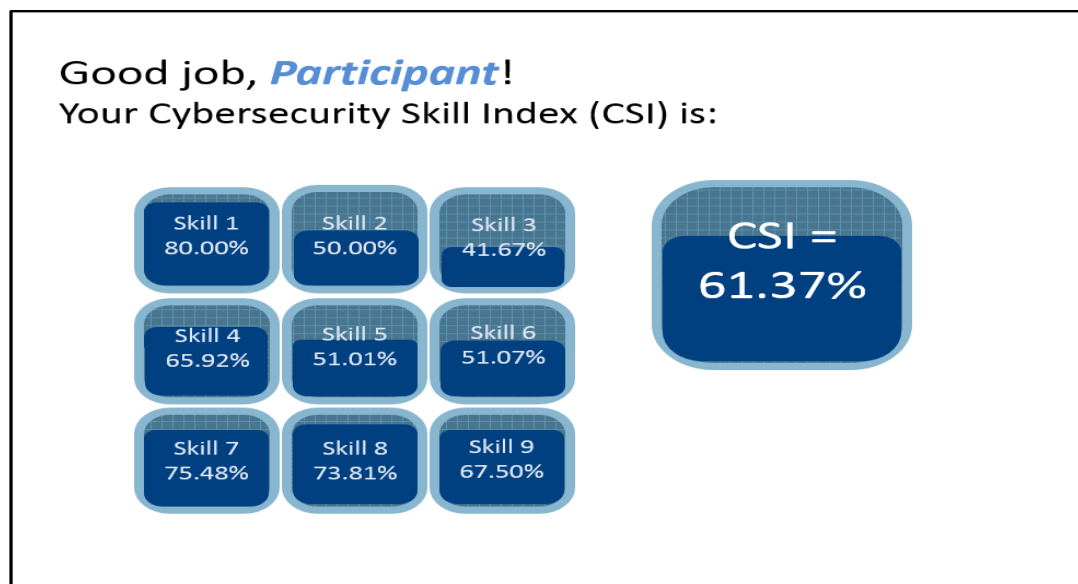
Rigorous testing was completed to ensure the validity and reliability of the cybersecurity threats situational assessment tool. Before beginning the validity testing, Institutional Review Board (IRB) approval was obtained to work with human subjects. Over the course of two days, 40 computer and mobile users employed at a public place of worship in the southeastern United States were emailed invitations to participate in the tool testing. The validity testing was conducted in a meeting room that was setup to emulate an office space with a laptop that displayed the cybersecurity threat situational tool in a Web browser. Each participant was made aware of the testing activities and given an opportunity to ask questions before signing a consent form. Of those emailed, 21 agreed to participate in the validity testing of the cybersecurity threats situational assessment tool, generating a 52.5% response rate.

The sessions began with each participant asked to interact with the cybersecurity threats situational assessment tool, while a research assistant observed the actions taken by the participant. Each participant was presented the top nine expert validated cybersecurity threats and assessed on their respective cybersecurity skills (Carlton & Levy, 2015; Carlton et al., 2015). A complete list of the skills assessed is shown in Table 1. The situational assessment tool presented each participant with four vignette-based realistic cybersecurity threats incrementing in difficulty. After each vignette was presented, the assessment tool required the participant to

respond to the presented cybersecurity threats to score their CySL. A total of 36 cybersecurity threat tasks, identified through literature (e.g., Symantec Corporation, 2018), were presented as a research assistant manually recorded the participant's hands-on activity (i.e. decision or action taken on the task presented) demonstrating their cybersecurity skills levels. At the conclusion of each participant's session, the research assistant then compared the manually recorded scores to the automatically recorded scores by the tool before beginning a new session with the next participant. At the conclusion of the third participant's session, a scoring anomaly was noted between the manually recorded score and that recorded by the situational assessment tool. The anomaly was corrected prior to the next session of the validity testing (Sheng et al., 2007). After all participant sessions were completed, the vignettes-based realistic cybersecurity threat situational assessment tool was deemed validated and reliable for collecting data in the empirical part of this research project.

**Table 1.** Top Nine Expert Validated Cybersecurity Skills (Carlton & Levy, 2015)

Skill 1	Preventing the leaking of confidential digital information to unauthorized individuals
Skill 2	Preventing malware via non-secure Websites
Skill 3	Preventing personally identifiable information (PII) theft via access to non-secure networks
Skill 4	Preventing PII theft via e-mail phishing
Skill 5	Preventing malware via e-mail
Skill 6	Preventing credit card information theft by purchasing from non-secured Websites
Skill 7	Preventing information system compromise via USB or storage drive/device exploitations
Skill 8	Preventing unauthorized information system access via password exploitations
Skill 9	Preventing PII theft via social networks
CSI	Overall Cybersecurity Skill Index



**Figure 1.** Sample Screen of The Participants' Average Scores Earned During Validity Testing (Displayed to the Participant at the End of the Final Session)



At the conclusion of the validity testing, the data collected was analyzed as a baseline in preparation for the follow-up empirical research. On average, the 21 participants completed the cybersecurity threats situational assessment tool within 33 minutes. The average scores of the 21 participants' individual skills and overall cybersecurity skills index (CSI) may be seen in Figure 1. This representation is similar to the one each participant received at the end of their session during the validity testing of the cybersecurity threats realistic situational assessment tool. Furthermore, as seen in Figure 1, the participant scored the highest, an average of 80%, at Skill 1, which is preventing the leaking of confidential digital information to unauthorized individuals. Whereas, the average score for Skill 3, preventing Personal Identifiable Information (PII) theft via access to non-secure networks, was the lowest (41.67%), although scores ranged from 10% to 100%. In addition, the data revealed the lowest overall CSI score was 39.04% with the highest score of 73.63%. Whereas, the average overall CSI score was 61.37%. Further analysis of the data was not conducted as the focus of this phase of the larger research project was to provide knowledge sharing of the process we have conducted to ensure the validity and reliability of the cybersecurity threats situational assessment tool.

## **Conclusions**

### **Discussion**

Due to the intensity of cybersecurity attacks over time, organizations are increasing the priority of cybersecurity skills due to financial and information losses caused by insiders, but often remain unprepared to address cybersecurity attacks (PricewaterhouseCoopers (PwC), 2018). This study built on prior research that defined cybersecurity skills as (i.e., preventing malware, PII, & WIS breaches) the combination of individuals' technical knowledge, ability, and experience surrounding the hardware as well as software required to execute IS security to mitigate cybersecurity attacks (Boyatzis & Kolb, 1991; Carlton & Levy, 2015; Choi et al., 2013). Thus, the need for a cybersecurity threats situational assessment tool that does not result in financial and information losses is paramount to organizations as well as academia research. The key focus of this study is to share some of the knowledge related to the process of designing a robust hands-on cybersecurity threat situational tool.

The outcome of this study is hoped to contribute notably to the body of knowledge and has several implications for providing researchers as well as practitioners insight into the developmental tools in the context of cybersecurity, while the processed overall can be adopted for other fields as well. Understanding an employee's CySL is critical to securing information and the systems that stores it, as organizations continue to rely on the Internet for conducting their daily operations. Furthermore, this study validated that the CSI benchmarking index could be used to assess the hands-on CySLs of computer and mobile users based on their demonstrated skills on cybersecurity threat situational tasks (Carlton et al., 2015). Moreover, this study provides a roadmap for development and testing of robust tools to help bridge between applied research and industry when it comes to complex emerging issues. Cybersecurity threats situational assessment tool is one example that may be used to assess the CySLs of computer and mobile device users within an organization. The focus of developmental research is to design, develop, and empirically test tools that are robust in their abilities to assist organizations with

emerging challenges, while providing insight into what the organization can do to further mitigate threats or address emerging organizational challenges.

## **Limitations**

No research is clear of limitations, while this study included several limitations. The first limitation is the eight SMEs that were engaged in the review and commenting of the blueprint of the skills, four vignette-based realistic cybersecurity threat per skill, and the scorings that goes along with it. While the sample of eight may appear small, the use of two Delphi processes and the length of the blueprint for the tool itself, took SMEs over two hours to conduct each review. Thus, although eight SMEs appear to be a small sample, the depth of the review, as well as dedication of these SMEs to the validity and reliability of the tool by their constructive comments demonstrated to be much valuable. A second limitation is that the tool was developed in the context of organizations in the United States, while every effort was made to ensure the tool is country and culturally natural, it is a limitation. A third limitation is that the tool includes three skills that are within the context of the workplace, so individuals who have never worked or are retired may score lower on those skills due to lack of (or recent) experience in the workplace.

## **Future Research**

The areas for future work in cybersecurity skills assessment appear numerous, given that it serves as the foundation for cybersecurity threat mitigations. Furthermore, the future of cybersecurity has broad implications due in part to the rapid pace of technological development (PwC, 2018). First, an empirical study that includes the cybersecurity threats situational assessment tool is warranted with a very larger group of participants to ensure a baseline is established with understanding of segments of the population that are above or below the baseline. Moreover, additional future research would increase the validity of the cybersecurity threats situational assessment tool, while allowing for investigation into various effects on the CySLs of individuals including their motivation to self-educate themselves about ways to mitigate emerging cybersecurity threats. Last, the cybersecurity threats situational assessment tool may be used by researchers and industry to assess as well as provide awareness regarding CySs. In addition, Security Education, Training, and Awareness (SETA) programs may include the tool to assess and aide in the mitigation of cybersecurity threats.

## **References**

- Alias, N. A. (2015). Designing, developing and evaluating a learning support tool: A case of design and development research (DDR). Retrieved from Sage Research Methods website: <http://srmo.sagepub.com/view/methods-case-studies-2015/n14.xml?rskey=q0vTAG&row=1th>
- Ball, A., Ramim, M. M., & Levy, Y. (2015). Examining users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems. *Online Journal of Applied Knowledge Management*, 3(1), 180-207.



- 
- Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly*, 25(1), 1-16.
- Boyatzis, R. E., & Kolb, D. A. (1991). Assessing individuality in learning: The learning skills profile. *Educational Psychology*, 11(3/4), 279-295.
- Brown, S. D., Levy, Y., Ramim, M. M., & Parrish, J. (2015). Pharmaceutical companies' documented and online privacy practices: Development of an index measure and initial test. *Online Journal of Applied Knowledge Management*, 3(2), 68-88.
- Cybersecurity Curricula 2017 (2017). Curriculum guidelines for post-secondary degree programs in cybersecurity. Available from <http://cybered.acm.org/>
- Carlton, M., & Levy, Y. (2015). Expert assessment of the top platform independent cybersecurity skills of non-IT professionals. *Proceedings of the 2015 IEEE SoutheastCon*, Ft. Lauderdale, Florida, pp. 1-6. doi:10.1109/SECON.2015.7132932.
- Carlton, M., Levy, Y., Ramim, M. M., & Terrell, S. R. (2015). Development of the MyCyberSkills™ iPad app: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills. *Proceedings of the Pre-International Conference on Information Systems (ICIS) SIGSEC - Workshop on Information Security and Privacy (WISP) 2015*, Ft. Worth, Texas.
- Creswell, J. W. (2005). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research (2nd ed.)*. Upper Saddle River, NJ: Pearson.
- Chakhssi, F., de Rulter, C., & Bernstein, D. (2010). Reliability and validity of the Dutch version of the behavioural status index: A nurse-rated forensic assessment tool. *Assessment*, 17(1) 58.69.
- Choi, M. S., Levy, Y., & Hovav, A. (2013). The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. *Proceedings of the Pre-International Conference on Information Systems (ICIS) SIGSEC – Workshop on Information Security and Privacy (WISP) 2013 (Paper 29)*, Milan, Italy. Retrieved from <http://aisel.aisnet.org/wisp2012/29>.
- Cox, C. (2015). Cyber capabilities and intent of terrorist forces. *Information Security Journal: A Global Perspective*, 24(1-3), 31-38.
- Ellis, T. J., & Levy, Y. (2010). A guide for novice researchers: Design and development research methods. *Proceeding of the Informing Science & Information Technology Education Conference (InSITE) 2010*, Casino, Italy, pp. 107-118.
- Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology* (6), pp. 323-337.
- Federal Bureau of Investigation (FBI). (2017). *Internet crime complaint center*. Retrieved from <https://www.ic3.gov/>

- 
- Geri, N., Winer, A., & Zaks, B. (2017). Challenging the six-minute myth of online video lectures: Can interactivity expand the attention span of learners? *Online Journal of Applied Knowledge Management*, 5(1), 101-111.
- Globes. (2016). Israel is a global cyber security power. <http://www.globes.co.il/en/article-israel-is-a-global-cyber-security-power-1001114556>.
- Helminen, A., Halonen, P., Rankinen, T., Nissinen, A., & Rauramaa, R. (1995). Validity assessment of a social support index. *Scandinavian Journal of Public Health*, 23(1) 66-74.
- Kissel, R. (2013). *Glossary of key information security terms* (NIST IR 7298 revision 2). Retrieved from National Institute of Standards and Technology website: <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>
- Leedy, P. D., & Ormrod, J. E. (2013). *Practical research: Planning and design* (10<sup>th</sup> Ed.). Upper Saddle River, NJ: Prentice Hall.
- Levy, Y., & Ramim, M. M. (2017). The e-learning skills gap study: Initial results of skills desired for persistence and success in online engineering and computing courses. *Proceeding of the Chais 2017 Conference on Innovative and Learning Technologies Research*, The Open University of Israel, Raanana, Israel, pp. 57E-68E. Retrieved from [http://www.openu.ac.il/innovation/chais2017/a1\\_2.pdf](http://www.openu.ac.il/innovation/chais2017/a1_2.pdf)
- McCallister, E., Grance, T., & Scarfone, K. (2010). *Guide to protecting the confidentiality of personally identifiable information (PII)* (NIST special publication 800-122). Retrieved from National Institute of Standards and Technology website: <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>
- Mendoza, V. D. (2014). *Measurement, tips, and errors: Making an instrument design in risk perception*. Retrieved from Sage Research Methods website: <http://srmo.sagepub.com/view/methods-case-studies-2014/n237.xml>.
- Nelson, J. A., Bustamante, R. M., Wilson, E. D., & Onwuegbuzie, A. J. (2008). The school-wide cultural competence observation checklist for school counselors: An exploratory factor analysis. *Professional School Counseling*, 11(4), 207-217.
- Onwuegbuzie, A. J., Bustamante, R. M., & Nelson, J. A. (2010). Mixed research as a tool for developing quantitative instruments. *Journal of Mixed Methods Research*, 4(1), 56-78.
- Paliszkievicz, J., Svanadze, S., & Jikia, M. (2017). The role of knowledge management processes on organizational culture. *Online Journal of Applied Knowledge Management*, 5(2), 29-44.
- PricewaterhouseCoopers (PwC). (2018). *The global state of information security survey 2018: Strengthening digital society against cyber shocks*. Retrieved from <https://www.pwc.com/us/en/cybersecurity/information-security-survey.html>.

- 
- Ramim, M. M., & Lichvar, B. T. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management*, 2(1), 122-136.
- Reinard, J. C. (2006). *Communication research statistics*. Thousand Oaks, CA: Sage Publications, Inc.
- Richey, R. C., & Klein, J. D. (2014). Design and development research. In: Spector, J., Merrill, M., Elen, J., & Bishop, M. (Eds.) *Handbook of Research on Educational Communications and Technology*. New York, NY: Springer.
- Rogers, T. B. (1995). *The psychological testing enterprise: An introduction*. Pacific Grove, CA: Brooks/Cole Publishing Company.
- Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., & Cranor, L. F. (2007). *Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish*. Retrieved from Carnegie Mellon University Research Showcase website: <http://repository.cmu.edu/isr/22/>.
- Solek-Borowska, C. (2017). Knowledge creation processes in small and medium enterprises: A Polish perspective. *Online Journal of Applied Knowledge Management*, 5(2), 61-75.
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, 13(2), 147-169.
- Symantec Corporation. (2018). *Internet security threat report*, 23. Retrieved from <https://www.symantec.com/security-center/threat-report>
- Tracey, M. W. (2009). Design and development research: A model validation. *Educational Technology, Research and Development*, 57(4), 553-571.
- Tracey, M. W., & Richey, R. C. (2007). ID model construction and validation: A multiple intelligences case. *Educational Technology, Research and Development*, 55(4), 369-390.
- U.S. Department of Labor, Bureau of Labor Statistics. (2018). *Occupational outlook handbook*. Retrieved from <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm>.
- United Kingdom. (2015, November). *National security strategy and strategic defence and security review 2015* (Cm 9161). Retrieved from [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/478933/52309\\_Cm\\_9161\\_NSS\\_SD\\_Review\\_web\\_only.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf)
- Wang, Q., Nieveen, N., & van den Akker, J. (2007). Designing a computer support system for multimedia curriculum development in Shanghai. *Educational Technology Research and Development*, 55(3), 275-295.

### **Authors' Biographies**

**Dr. Melissa Carlton** completed her doctoral studies in Information Systems and Cybersecurity at the College of Engineering and Computing (CEC) at Nova Southeastern University (NSU). She has presented and published in top-tier peer reviewed publications. Her service to the

---

academic community includes ad hoc reviewer/editor, student mentor, as well as co-coordinator and presenter of cybersecurity skills to 200 Miami-Dade high school students as part of Cybersecurity Awareness Day at NSU. She is a member of Levy CyLab, Association for Computing Machinery (ACM), Association for Information Systems (AIS), Institute of Electrical and Electronics Engineers (IEEE), and Upsilon Pi Epsilon honor society.

**Dr. Yair Levy** is a Professor of Information Systems and Cybersecurity at the College of Engineering and Computing at Nova Southeastern University, the [Director of the Center for Information Protection, Education, and Research \(CIPHER\)](#), and chair of the Information Security Faculty Group at the college along with serving as the director of the M.S. and Ph.D. programs in Cybersecurity and Information Assurance. He heads the Levy CyLab (<http://CyLab.nova.edu/>), which conducts innovative research from the human-centric lens of key research areas Cybersecurity, social engineering, cyber threat mitigation, and skills. Levy authored one book, three book chapters, and numerous peer-reviewed journal as well as conference proceedings publications. His scholarly research have cited over 3,000 times. Dr. Levy has been an active member of the US Secret Service (USSS)'s - Miami Electronic Crimes Task Force (MECTF) and The South Florida Cybercrime Working Group (SFCWG). He was trained by the Federal Bureau of Investigation (FBI) on various topics, and actively serves as a board member on of the South Florida FBI/InfraGard, and consults federal agencies, state and local government groups on cybersecurity topics. He is also a frequent invited keynote speaker at national and international meetings, as well as regular media interviews as a Subject Matter Expert (SME) on cybersecurity topics. Read more about Dr. Levy via: <http://www.nova.edu/~levyy/>

**Dr. Michelle M. Ramim** is a part-time professor at the Middle Georgia State University. She has extensive experience in information technology (IT) consulting. Dr. Ramim directed the development and implementations of several IT projects including promotional and interactive websites for major enterprises such as Debeer (Diamond Trading Company). Her current research interests include ethical issues with IT, cybersecurity and crisis management, privacy and legal aspects of computing, as well as cybersecurity in healthcare. She has published articles in peer-reviewed outlets including journals, conference proceedings, encyclopedias, and an invited chapter. A number of her papers won the 'best paper' award in national and international peer-review conference proceedings. Moreover, she has been serving as a referee reviewer for national and international scientific journals, conference proceedings, as well as management information systems textbooks. She has developed the supplemental material for the Pearson and Saunders (2012) 5th ed. Book "Managing and Using Information Systems: A Strategic Approach" by Wiley & Sons. She earned her Bachelor's degree from Barry University in Miami, Florida. Dr. Ramim has received her Executive MBA from Florida International University. She completed her Ph.D. in Information Systems at the College of Engineering and Computing, Nova Southeastern University.